

# Phil Buckley (TS/SCI)

## Cybersecurity Engineer II, IAM II, IAT II, IASE I

San Diego, CA 92025 - 661-444-1816 - phil@phillipbuckley.com - www.linkedin.com/in/pmbuckley

---

### EXECUTIVE SUMMARY

Experienced Cybersecurity professional and retired U.S. Navy Submarine NCO IT specialist with over 25 years of combined military and civilian service in Information Systems and Cybersecurity. Fully trained and capable of performing as a Navy Qualified Validator (NQV) II, with extensive hands-on experience at all steps in the RMF process, and compliance across DoD and DON environments. Proficient in tools including ACAS, Enterprise Mission Assurance Support Service (eMASS), Evaluate-STIG, STIG Viewer, and Xacta, with a proven track record supporting ATO efforts for classified and SAP systems.

Currently delivering direct cybersecurity support to five Naval Information Warfare Center (NIWC) Pacific Special Access Programs (SAP), including Foreign Military Sales (FMS) and fleet-essential projects. Skilled in translating complex cybersecurity requirements into actionable security controls and collaborating across engineering, operations, and leadership teams to achieve mission success. Adept at preparing and presenting Information Assurance (IA) assessments and recommendations to technical and executive stakeholders. Lauded by Naval Intelligence Activity (NIA) for producing an RMF package with the lowest POA&M items in recent history and for maintaining security-first development processes.

Seeking a Security Engineer role where I can apply my in-depth cybersecurity knowledge and leadership experience in support of high-impact DoD and DON initiatives. Committed to fostering a collaborative environment, breaking down information silos, and enabling compliance with DoD, DON, National Institute of Standards and Technology (NIST), and civilian cybersecurity standards—while actively pursuing formal Navy Validator certification.

---

### PROFESSIONAL SKILLSET

<b>RMF Expertise</b>	Extensive experience with RMF processes and security authorization packages.
<b>Security Control Assessments</b>	Proficient in assessing and documenting security controls, performing risk assessments, and recording compliant and failed security controls in eMASS and Xacta.
<b>eMASS and Xacta Proficiency</b>	Skilled in using eMASS and Xacta databases for recording security control compliance and generating Security Assessment Reports (SAR).
<b>Validation Services</b>	Adept at providing validation services and sustainment support for DoD and DON IT systems and networks.
<b>Traceability of Vulnerabilities</b>	Expertise in ensuring traceability of vulnerabilities from raw assessment results to the POA&M.
<b>DoD Security Control Assessments</b>	Adept in conducting DoD Security Control assessments and RMF processes.

---

### TECHNICAL PROFICIENCIES, SKILLS & COMPETENCIES

<b>Computer Network Defense (CND) &amp; IA</b>	Versed in using eMASS and Xacta for recording security control compliance and generating Security Assessment Reports (SAR). Experienced in conducting DoD Security Control assessments and RMF processes, IAVM (e.g., IAVA, IAVB) Program, Special Access Programs (SAP), Two-Factor/Multifactor Authentication (2FA/MFA)
<b>Cybersecurity Tools &amp; Software</b>	eMASS, eMASster, ESS/HBSS (McAfee/Trellix ePolicy Orchestrator (ePO) Server), SCAP Workbench, STIG Viewer, Tenable Security Center (Tenable.SC) and Nessus, Xacta
<b>General Tools &amp; Software</b>	Apache JBoss, Apache Tomcat, Docker, firewall configuration (hardware & software), Jira, Kubernetes, Linux/UNIX BASH Shell Script, MS Exchange Server, MS Office (Access, Excel, PowerPoint, Project, Word), MS PowerShell, MS Project, MS SQL, MS Visio, MS VBA, MS Windows Batch Script, MS WSUS, Postgres/PostgreSQL, switch and router configuration (e.g., Brocade, Cisco IOS, Dell), VMware vCenter, VMware vSphere
<b>Operating Systems</b>	CentOS (7-9), Fedora (all), MS Windows Server (all), MS Windows Workstation (all), Red Hat Enterprise Linux (RHEL) (all), Ubuntu (18-24), VMware ESXi (6.5, 7.x)

**DEGREES & APPRENTICESHIPS**

- Degrees**
  - B.A. Management**, National University, San Diego CA (In Progress)
  - A.A. Electronics Technology**, Coastline Community College, Fountain Valley CA (2018)
  - A.A. Information Systems**, Coastline Community College, Fountain Valley CA (2018)
  - A.A. Supervision and Management**, Coastline Community College, Fountain Valley CA (2018)
- Apprenticeships**
  - Computer Programmer**, United States Military Apprenticeship Program (USMAP) (2020)

**CERTIFICATIONS & CLEARANCES**

- Certifications**
  - CompTIA** - Security+ Continuing Education (CompTIA Sec+ CE)
  - CompTIA** - A+ IT Technician (CompTIA A+ IT Technician)
  - VMware** – Certified Associate 6 – Data Center Virtualization (VMware VCA6-DCV)
  - ISC<sup>2</sup>** – CISSP (expired) (actively pursuing, ETC 08/2025)
  - US Navy** – Navy Qualified Validator (NQV) (training and experience complete), ETC ASAP)
- Clearances**
  - TS/SCI(eligible)** – “Cleared for TOP SECRET information and granted access to Sensitive Compartmented Information (SCI) based on a completed T5/T5R investigation and admittance to the Continuous Monitoring program.”

**PROFESSIONAL EXPERIENCE**

**EPSILON C5I, INC.** – San Diego CA

2022-Present

**Cybersecurity Engineer II**

Primary cybersecurity engineer for the core components of a shore (schoolhouse learning suite) and a shipboard-based training suite, and three Naval Information Warfare Center (NIWC) Pacific Special Access Program (SAP) projects. Provides status updates and body of evidence (BoE) documentation to project managers on a routine basis. Develops detailed instructions, procedures, and policies related to the installation, configuration, and maintenance of cybersecurity software to include Assured Compliance Assessment Solution (ACAS) (i.e., Tenable.sc, Nessus), Host-Based Security Solution (HBSS)/Enterprise Security Solution (ESS) (i.e., McAfee/Trellix ePolicy Orchestrator On-Premises (ePO On-Prem)), Security Technical Implementation Guide (STIG) Viewer, Security Content Automation Protocol (SCAP) Compliance Checker (SCC) scanning tool, and Evaluate-STIG compliance scanning tool. Maintains Risk Management Framework (RMF) packages in eMASS and Xacta databases ensuring accurate, up-to-date documentation and compliance. Conducts security control assessments and risk assessments, recording results in eMASS and generating Security Assessment Reports (SAR).

**Key Contributions**

- Drove to completion an Authorization to Operate (ATO) package for a major Program Manager, Warfare 120 (PMW-120) fleet training system.
- Implemented remediation & compliance measures obtaining near 100% compliance with Naval Intelligence Activity (NIA) requirements for a SAP SIGINT training suite.
- Generated BoE documentation obtaining Interim Authority to Test (IATT) certifications for three major NIWC Pac projects.
- Promoted a collaborative environment where engineers, technical writers, and cybersecurity specialists continually assist each other with solutions to encountered issues while maintaining compliance with cybersecurity requirements.
- Directly assisted with the installation and cybersecurity inspection of a primary schoolhouse SIGINT program in preparation for the roll-out of an additional six schoolhouse implementations.

## Phil Buckley (TS/SCI)

Professional Experience (Con't)

GROVE RESOURCE SOLUTIONS, INC. (GRSI) – San Diego CA

2021-2022

### Cybersecurity Analyst/System Administrator

Primary cybersecurity analyst for two NIWC Pac Special Access Program (SAP) SIGINT projects and one platform status monitoring project for planned delivery to the US Navy. Build and maintain two compliance scanning virtual appliances. Provided status updates and body of evidence (BOE) documentation to project managers on a routine basis.

#### Key Contributions

- Conducted ACAS (Tenable.sc, Nessus) and SCAP/STIG compliance scans against 15 RHEL 7 and RHEL 8 VMs across two blade servers and assisted with remediation and compliance measures to obtain near 100% compliance.
- Provided software control board documentation (SCIS) for planned changes to Program of Record (POR) systems.
- Authored documentation to obtain interim authority to test (IATT) utilizing the NIWC Pac LITE Process.
- Created necessary BOE documentation to obtain IATT certifications for two major NIWC Pac projects.

USS COLUMBIA (SUBMARINE) – Pearl Harbor HI

2018-2020

### Information Assurance Manager/System Administrator/Division Lead

Direct a division of 12 personnel to investigate security breaches and other security incidents supporting Electronic Warfare and Information Technology environments. Establish security measures and maintain software to protect systems and information infrastructure, including Enterprise Application Integration (EAI). Install security software on Classified and Unclassified Windows networks, Anti-virus, Web Applications, and firewalls. Ensure compliance with current IAVM guidance. Monitor server, firewall, intrusion detection, and network traffic logs for anomalous and/or suspicious activity. Endorse security enhancements to improve the security posture of the organization. Manage Special Access Programs (SAP).

#### Key Contributions

- Migrated classified and unclassified Windows network from operational submarine to living barge with zero downtime.
- Designed and programmed several databases and spreadsheets for asset and message tracking.
- Developed and implemented 25 automation scripts to improve server performance and data efficiency.

NAVAL SUBMARINE SUPPORT COMMAND – Pearl Harbor HI

2014-2018

### Department Manager/Information Assurance Manager/System Administrator

Develop, implement, and maintain an IT Security Risk Management program. Create and audit policies and procedures for IT Security Risk Management to ensure compliance with regulatory standards with a keen focus on improving efficiency. Design and supervise the replacement of two Navy & Marine Corps Intranet (NMCI) 400 node networks, providing the most modern network available to two US Pacific Fleet submarine squadrons and support command.

#### Key Contributions

- Reduced transient sailors' onboarding time by 75% and saved annual expenses by designing a database to manage an average annual throughput of 2000 transient and permanent staff personnel.
- Resolved seven security incidents while ensuring compliance with federal and civilian information assurance and compliance directives and best practices.

---

## ADDITIONAL PRIOR EXPERIENCE

*Information Assurance Manager/System Administrator/Division Lead/EKMS Manager/Database Designer, Administrator  
at USS LA JOLLA (Submarine) – Pearl Harbor, HI 2010-2014*

*Site Lead/Primary Instructor/Curriculum Developer/Information Assurance Manager/System Administrator  
Center for Information Dominance – Bangor, WA 2006-2010*

*Information Assurance Manager/Network Administrator/Division Lead/Database Designer  
USS ALABAMA (Submarine) – Bangor, WA 2002-2006*

*U.S. Naval Basic Training, ET COMMS "A" School, Submarine School, ET Submarine Radioman "A" & "C" School  
North Chicago, IL, Groton, CT, Bangor, WA 2000-2002*

*Distance Support Technician/Database Designer/Technical Mentor  
Microsoft Corporation, Stream International – Beaverton OR 1998-1999*